

VERIFIABLE, SECRET SHUFFLES OF ENCRYPTED DATA, SUCH AS ELGAMAL  
ENCRYPTED DATA FOR SECURE MULTI-AUTHORITY ELECTIONS

ABSTRACT

A cryptographic process permits one to *verifiably* shuffle a series of input data elements. One or more authorities or individuals "shuffle," or "anonymize" the input data (e.g. public keys in discrete log form or ElGamal encrypted ballot data). The process includes a validity construction that prevents any one or more of the authorities or individuals from making any changes to the original data without being discovered by anyone auditing a resulting proof transcript. The shuffling may be performed at various times. In the election example, the shuffling may be performed, e.g., after ballots are collected or during the registration, or ballot request phase of the election, thereby anonymizing the identities of the voters.

0931669-033404  
TOP SECRET